What is Claimed is:

1. A digital signature system comprising:

a database holding access control rules that identify documents authorized users are allowed to have electronically signed; and

a signing system capable of receiving signature requests from a plurality of authorized users, each signature request including a document to be signed, wherein said signing system parses the document to be signed and compares information obtained thereby to the access control rules stored in said database to determine whether the authorized user is authorized to have the document signed, and wherein if it is determined that the authorized user is authorized to have the document signed, the signing system signs the document using authentication information unique to the signing system.

2. A digital signature system as recited in claim 1, wherein the access control rules identify at least one of a type and attribute of documents each user is authorized to have signed.

3. A digital signature system as recited in claim 2, wherein the signing system parses the document to be signed to determine at least one of a type and attribute of the document and compares the determined type and attribute of the document to the access control rules stored in the database to determine whether the user is authorized to have the document signed.

4. A digital signature system as recited in claim 1, wherein the request further includes user authentication information unique to the requesting user, and wherein the signing system authenticates the user via the user authentication information and does not parse the document unless the user authenticates.

5. A digital signature system as recited in claim 4, wherein said user authentication information comprises a digital certificate, with corresponding public and private keys.

6. A digital signature system as recited in claim 5, wherein the digital certificate comprises an X-509 certificate.

7. A digital signature system as recited in claim 4, further comprising an email interface, wherein the signature request is in the form of an email from the user addressed to the signing system.

8. A digital signature system as recited in claim 7, wherein said user authentication information comprises a user's email address.

9. A digital signature system as recited in claim 8, wherein the signing system authenticates the user by comparing the user's email address to email addresses stored in the database.

10. A digital signature system as recited in claim 1, further comprising a document validation server capable of receiving document validation requests from a user requesting a signed document to be validated and determining whether the signed document is valid in response to the request.

11. A digital signature system as recited in claim 1, wherein after the document validation server signs the document, the signed document is electronically forwarded to the user so that the user can forward the signed document to the recipient.

12. A digital signature system as recited in claim 1, wherein after the document is signed, the signed document is emailed to the user.

13. A digital signature system as recited in claim 1, wherein after the document is signed,

the signed document is automatically electronically forwarded to a recipient.

14. A digital signature system as recited in claim 13, wherein the signed document is emailed to the recipient.

15. A method of digitally signing documents using a signing system comprising:

storing access control rules that identify documents authorized users are allowed to have electronically signed;

receiving a signature request from at least one user, the signature request including a document to be signed;

determining whether the user is authorized to have documents signed;

if the user is authorized, parsing the document to be signed;

comparing information obtained by the parsing to the stored access control rules to determine whether the authorized user is authorized to have the attached document signed; and

if it is determined that the authorized user is authorized to have the attached document signed, signing the document using authentication information unique to the signing system.

16. A method as recited in claim 15, wherein the access control rules identify at least one of a type and attribute of documents each user is authorized to have signed.

17. A method as recited in claim 16, wherein the parsing step parses the document to be signed to determine at least one of a type and attribute of the document and the comparing step compares the determined type and attribute of the document to the access control rules stored in the database to determine whether the user us authorized to have the document signed.

18. A method as recited in claim 15, wherein the request further includes user authentication information unique to the requesting user, and wherein the signing system

authenticates the user via the user authentication information and does not parse the document unless the user authenticates.

19. A method as recited in claim 18, wherein said user authentication information comprises a digital certificate, with corresponding public and private keys.

20. A method as recited in claim 19, wherein the digital certificate comprises an X-509 certificate.

21. A method as recited in claim 15, further comprising an email interface, wherein the signature request is in the form of an email from the user addressed to the signing system.

22. A method as recited in claim 21, wherein it is determined whether the user is an authorized user, by comparing a user's email address with a list of stored email addressed corresponding to authorized users.

23. A method as recited in claim 15, further comprising electronically forwarding the signed document to the user so that the user can forward the signed document to the recipient.

24. A method as recited in claim 15, further comprising emailing the signed document to the user.

25. A method as recited in claim 15, further comprising electronically forwarding the signed document to an end recipient.

26. A method as recited in claim 25, wherein the signed document is emailed to the end recipient.

27. A signing system for digitally signing documents comprising:

storing means for storing access control rules that identify documents authorized users are allowed to have electronically signed;

receiving means for receiving a signature request from at least one user, the signature request including a document to be signed;

determining means for determining whether the user is authorized to have documents signed;

parsing means for parsing the document to be signed if the user is authorized;

comparing means for comparing information obtained by the parsing means to the stored access control rules to determine whether the authorized user is authorized to have the attached document signed; and

signing means for signing the document using authentication information unique to the signing system if it is determined that the authorized user is authorized to have the attached document signed.

28. A system as recited in claim 27, wherein the access control rules identify at least one of a type and attribute of documents each user is authorized to have signed.

29. A system as recited in claim 28, wherein the parsing means parses the document to be signed to determine at least one of a type and attribute of the document and the comparing meansp compares the determined type and attribute of the document to the access control rules stored in the database to determine whether the user us authorized to have the document signed.

30. A system as recited in claim 27, wherein the request further includes user authentication information unique to the requesting user, and wherein the signing system authenticates the user via the user authentication information and does not parse the document unless the user authenticates.

31. A system as recited in claim 30, wherein said user authentication information

comprises a digital certificate, with corresponding public and private keys.

32. A system as recited in claim 31, wherein the digital certificate comprises an X-509 certificate.

33. A system as recited in claim 27, further comprising an email interface means, wherein the signature request is in the form of an email from the user addressed to the signing system.

34. A system as recited in claim 33, wherein it is determined by the determining means whether the user is an authorized user, by comparing a user's email address with a list of stored email addresses corresponding to authorized users.

35. A system as recited in claim 27, further comprising forwarding means for electronically forwarding the signed document to the user so that the user can forward the signed document to the recipient.

36. A system as recited in claim 27, further comprising email means for emailing the signed document to the user.

37. A system as recited in claim 27, further comprising means for electronically forwarding the signed document to an end recipient.

38. A system as recited in claim 37, wherein the signed document is emailed to the end recipient.

39. A digital signature system comprising:

database means for holding access control rules that identify documents authorized users are allowed to have electronically signed; and

signing means capable of receiving signature requests from a plurality of authorized

users, each signature request including a document to be signed, wherein said signing means parses the document to be signed and compares information obtained thereby to the access control rules stored in said database means to determine whether the authorized user is authorized to have the document signed, and wherein if it is determined that the authorized user is authorized to have the document signed, the signing means signs the document using authentication information unique to the signing means.